

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**A System and Method
for
Secure Third-Party Development and Hosting within a
Financial Services Network**

Inventor(s):
Vasantha Badari
Michael Waterston
Jarrod Pfost
Eric Jackstat

ATTORNEY'S DOCKET NO. MS1-428US

1
2 This application claims express priority to U.S. Provisional Application No.
3 60/TBD,TBD entitled *A System and Method for Secure Third-Party Development*
4 *and Hosting within a Financial Services Network* by Badari, et al. and filed on
5 January 21, 2000.

6
7 **TECHNICAL FIELD**

8 This invention generally relates to electronic bill presentment and payment
9 (EBPP) systems and, more particularly, to system and method for secure third-
10 party content development and hosting within a financial services network.

11
12 **BACKGROUND**

13 The concept of buying goods on “credit”, or a promise for future payment,
14 is not new. Today, nearly everyone in the industrial world is familiar with
15 receiving bills for goods and services. Every month, like clockwork, millions of
16 consumers receive bills for goods and services. For convenience, the term
17 “consumer” is used throughout this document to represent both a typical person
18 who consumes goods and services as well as a business that consumes goods and
19 services.

20 At the end of each billing cycle, a biller typically generates a bill or
21 statement for each consumer account having a positive or negative account
22 balance, or having transactions that yielded a zero balance. As used herein, a
23 “biller” is any party that originates billing statements for goods or services
24 rendered to the consumer. Examples of billers are utilities, government,
25 merchants, and intermediate billing services such as banks. The printed billing
statement is typically customized according to the biller’s preferences. For

1 example, it is common for billing statements to be printed on colored paper,
2 display the biller's logo, provide a billing summary, and show itemized
3 transactions. This information is organized in a custom format that is unique to
4 and controlled by the biller.

5 The biller also creates remittance information that associates the consumer
6 account with the bill and any payment toward the bill. The remittance information
7 is typically in the form of a detachable stub or coupon that the consumer detaches
8 from the billing statement and returns along with the payment. This remittance
9 stub is also customized according to the biller's preferences.

10 Recently, electronic bill presentment and payment (EBPP) systems have
11 been developed to automate this process of bill delivery and payment. Companies
12 such as Microsoft, Checkfree and Visa, Inc. are developing products in this space,
13 the result of which heretofore has been an associated number of closed,
14 proprietary EBPP systems. One such system is described in U.S. Patent No.
15 5,465,206, entitled "Electronic Bill Pay System," which issued November 7, 1995
16 and is assigned to Visa International.

17 The Visa bill payment system permits bills to be sent by billers to
18 consumers via U.S. mail or electronically via email. Unfortunately, the Visa
19 system suffers from a number of drawbacks. First, the email message containing
20 the bill must conform to requirements imposed by Visa. This requirement stems
21 from the need to route remittance information back to the biller through the
22 VisaNet® network (one of the four Automated Clearing Houses (ACH) used by
23 financial institutions to clear transactions between financial institutions). Thus,
24 the biller has little or no control over the format concerning how the bill is
25 presented to the customer, but must instead accommodate a format compatible
with this network.

1 Second, the Visa system is designed to support the presentment of “bills”
2 from corporate billers, and would not accommodate the myriad of financial
3 transactions conducted among and between consumers. Third, these prior art
4 EBPP systems (e.g., Visa, Checkfree, etc.) have not be designed for
5 interoperability. Currently, there is no solution available to integrate all of the
6 users from these disparate EBPP systems into a common, ubiquitous network.

7 These limitations are significant in a number of respects, the most notable
8 of which are the cost and responsiveness of such prior art electronic financial
9 systems. Moreover, the biller must provide the Visa system with a significant
10 amount of information, which the consumer would likely deem to be confidential.
11 Many billers do not typically wish to share this information with third parties (e.g.,
12 the Visa system) for fear that the confidential information may be breached,
13 resulting in fraud.

14 Recently, communication protocols have been introduced, i.e., the Open
15 Financial Exchange (OFX) and, more recently the Internet Financial Exchange
16 (IFX), as a means through which the disparate, proprietary financial networks can
17 communicate with one another. While these protocols enable billers and financial
18 networks to communicate among one another, it does not provide a framework
19 which enables billers to develop content within the financial networks. While it is
20 known that some EBPP systems enable a biller to customize the billing statement
21 presented to the consumer, it does not provide the biller with unilateral control
22 over the content and format of the bill. Rather, these prior art systems provide the
23 billers with a “template”, which the biller can populate to generate their
24 “customized” bill. The problem, however, is that while the content is unique to
25 the individual biller, the form is not. Quite simply, none of the prior art EBPP
systems enable a biller to develop or host their own content, accessible on or
through the EBPP system.

1 Thus, a system and method for secure third-party content development and
2 hosting within a financial services network is required, unencumbered by the
3 limitations commonly associated with prior art development and presentment
4 architectures. Just such a solution is provided below.

5 6 7 **SUMMARY OF THE INVENTION**

8 This invention concerns a system and method for secure third-party content
9 development and hosting within a financial services network. According to a first
10 aspect of the present invention, an electronic billing statement is presented as a
11 user interface to a registered user of a server, the electronic billing statement
12 comprising a first component, hosted by a financial service center, to navigate the
13 user UI and invoke one or more functions of the financial service center, and a
14 second component, hosted by a third-party, to provide detailed billing information
15 from a biller to the registered user.

16 17 **BRIEF DESCRIPTION OF THE DRAWINGS**

18 The same reference numbers are used throughout the figures to reference
19 like components and features.

20 **Fig. 1** is a diagrammatic illustration of a data network incorporating the
21 teachings of the present invention;

22 **Figs. 2A and 2B** provide alternate embodiments of a secure content
23 development system incorporating the teachings of the present invention;

24 **Fig. 3** is a block diagram of a computer system offering the features of the
25 secure development system, according to one embodiment of the invention;

1 **Figs. 4A and 4B** illustrate block diagrams of alternate embodiments of a
2 third-party content development system, suitable for use within the data network
3 of Fig. 1;

4 **Fig. 5** illustrates a block diagram of an example computer system suitable
5 for use to develop content within the third-party content development system of
6 Fig. 5;

7 **Fig. 6** graphically represents an example data structure to store
8 authentication codes and bill data facilitating a seamless transition between the
9 financial service center and the biller to present the user with requested bill detail;

10 **Fig. 7** is a flow chart of an example method facilitating third-party content
11 development within the financial service center of Fig. 1;

12 **Fig. 8** graphically illustrates an example user interface provided by the
13 secure development system enabling a biller to establish and manage a
14 development account on the system;

15 **Fig. 9** graphically represents an example user interface provided by the
16 secure development system enabling a biller administrator to create a development
17 certification for a developer to use the secure development system;

18 **Fig. 10** graphically illustrates an example user interface enabling a biller to
19 customize their presence on the financial service center to utilize their own custom
20 developed content;

21 **Fig. 11** is a flow chart of an example automated validation method to
22 validate the integrity of third-party developed content before it is propagated
23 beyond a working directory of the secure development system;

24 **Fig. 12** is a flow chart of an example method for utilizing third-party
25 developed and/or hosted content within the financial service center;

Fig. 13 is an architectural representation of a financial service center
presenting a consumer with content including a financial service center component

1 and a third-party developed and/or hosted component, according to the teachings
2 of the present invention;

3 **Fig. 14** graphically illustrates an example bill summary page, according to
4 one embodiment of the present invention; and

5 **Fig. 15** illustrates an example bill detail page, according to one
6 embodiment of the present invention.

7 **DETAILED DESCRIPTION**

8 This invention concerns a system and method facilitating personal
9 electronic financial transactions with anyone, including non-users of the system
10 and methods, via an email system. In this regard, the present invention overcomes
11 a number of the limitations commonly associated with the prior art including, in
12 particular, the aggregation problem. It will be appreciated, from the description to
13 follow, that the present invention builds upon an innovative electronic bill
14 presentment and payment system first described in presently pending U.S. Patent
15 Application No. 09/XXX,XXX, which is a continuation of U.S. Patent Application
16 No. 08/734,518 (now USP Z,ZZZ,ZZZ), entitled *Electronic Bill Presentment and*
17 *Payment System* filed on TBD by Remmington, et al., the disclosure of which
18 being expressly incorporated herein by reference. In describing the present
19 invention, example network architectures and associated methods will be
20 described with reference to the above drawings. It is noted, however, that
21 modification to the architecture and methods described herein may well be made
22 without deviating from the present invention. Indeed, such alternate embodiments
23 are anticipated within the scope and spirit of the present invention.

24 **EXAMPLE SYSTEM ARCHITECTURE**

25 **Example Data Network**

1 **Fig. 1** illustrates an example network 100 including an innovative financial
2 service center 102 including a secure third-party content development system 116.
3 The secure third-party development system 116 enables third-parties (e.g., billers,
4 technical consultants for billers, etc.) to develop content (e.g., application server
5 pages), which is provided to consumers through the innovative FSC 102. Unlike
6 prior art EBPP systems, the secure third-party development system 116 provides
7 billers with substantial control over the form and substance of content provided to
8 consumers via the FSC 102 by allowing the billers to author and/or host a portion
9 of the content provided to the consumers.

10 With continued reference to Fig. 1, network 100 is comprised of a number
11 of network participants including consumers 104(a)...(n), billers/businesses
12 106(a)...(n), and financial institutions 108(a)...(n) each communicatively coupled
13 to the FSC 102 via one or more networks 110 and 112. As used herein, networks
14 110 and 112 are intended to represent a wide variety of networks and
15 communication technologies. In this regard, networks 110 and 112 may well
16 comprise, for example, public networks (Internet), private networks (enterprise
17 wide area networks (WAN)), data networks and communication networks (public
18 switched telephony network (PSTN), cellular telephony network, and the like). In
19 this regard, network 100 is intended represent a composite of any number of
20 networks through which participants can access and benefit from the innovative
21 services of FSC 102. Due to the confidential nature of the information and
22 transactions, however, security measures are taken when communicating over
23 public networks. According to one embodiment, for example, when the user is
24 communicating with the FSC 102 via the Internet, FSC 102 employs the well
25 known secure HyperText Transfer Protocol (HTTPS).

It will be appreciated that each of the network participants accesses and
utilizes the resources of network 100 through a computing platform. Accordingly,

1 consumers 104(a)...(n) are depicted communicative coupled to network 100 via
2 computing devices 114(a)...(n), respectively. Similarly, businesses 106(a)...(n),
3 financial institutions 108(a)...(n), and third-party content developer 126 also
4 access the resources of network 100 through one or more computing devices. For
5 ease of illustration and explanation, the computing interface for billers/businesses
6 106, financial institutions 108 and third-party content developer 126 have been
7 omitted from Fig. 1 so as to not obscure the innovative aspects of the present
8 invention. For purposes of this discussion, use of the term "consumer", "business",
9 "financial institution", "user" or "network user" are each intended to represent the
10 respective entity as well as a suitable computing interface.

11 As used herein the computing devices used by network users are intended
12 to represent a broad range of computing devices known in the art. As will be
13 shown with reference to Fig. 5, a computing device, e.g., 114, does not require any
14 special features or capability other than a browser to access and utilize the features
15 of FSC 102. Similarly, any number of typical personal computer systems may
16 well be used to develop content for publication via FSC 102 using any of a
17 number of well known application server pages (ASP) development tools such as,
18 for example, FrontPage 2000 offered by Microsoft Corporation of Redmond,
19 Washington. In this regard, computing devices 114(a)...(n) are intended to
20 include, but are not limited to, personal computers, electronic kiosks, personal
21 digital assistants (PDAs), wireless telephones, wireline telephones, thin-client
22 terminals, and the like through which a user may interact with email system 102.

23 FSC 102 is introduced in Fig. 1 as comprising the secure development
24 system 116, a storage device 118 to store and maintain administrative and
25 transactional information, and a consumer user interface 120. According to one
implementation, to be described more fully below, FSC 102 is implemented using
one or more computer systems, or data servers, which work in cooperation to

1 provide the innovative services described herein. It will be appreciated, from the
2 discussion to follow, that the innovative aspects of the FSC 102 may well be
3 embodied in hardware, e.g., analog or digital circuitry, or in software executed by
4 one or more processor(s) of the computer system(s) to implement the described
5 functions.

6 As will be developed more fully below, secure third-party development
7 system 116 enables a developer to write and automatically validate content for
8 publication to consumers through FSC 102. According to one aspect of the
9 invention, the developed content may also redirect an accessing consumer's
10 browser (or other user interface executing on a computing platform) to render
11 content hosted from a billers computer system(s) 106. That is, the secure third-
12 party development system 116 enables billers to author and/or host their own
13 content for publication through FSC 102.

14 As introduced above, storage medium 118 stores and maintains
15 administrative and transaction information for use by FSC 102. As will be
16 described in greater detail below, the administrative information may well contain
17 a plethora of information regarding the biller, consumers and their accounts, and
18 third-party developers. The transactional information provides a consumer with
19 bill summary information, payment information, status information and the like.
20 As used herein, storage medium 118 is intended to represent any of a number of
21 mass storage devices including, but not limited to, magnetic hard disk drive(s),
22 optical disk drives, compact disk (CD) read-only memory (ROM) drives, digital
23 versatile disk (DVD) drives, redundant array of inexpensive disk (RAID) systems,
24 tape drives, and the like. Moreover, although depicted as a single database within
25 a single storage device 118, it will be appreciated that FSC 102 may utilize a
number of storage mediums 118 comprising a plurality of databases to maintain
administrative and transactional information.

1 Consumer user interface (UI) 120 is intended to represent any of a broad
2 category of means by which a consumer can access and utilize the financial
3 transaction features of FSC 102. According to one embodiment, consumer UI 120
4 is a web page with links that enable a registered user to access and manage
5 financial accounts and conduct financial transactions with anyone (e.g., registered
6 user's and non-user's alike). According to the teachings of the present invention,
7 secure third-party development system 116 enables billers to create and/or host
8 content presented to a consumer via the consumer UI 120. Although described
9 with respect to a graphical, web based UI, it is to be appreciated that alternate UI's
10 may well be utilized without deviating from the scope and spirit of the present
11 invention.

12 As shown, billers/businesses 106(a)...(n) may access (and be accessed
13 from) FSC 102 via the network in any of a number of alternate means. According
14 to one implementation, business 106(a) may utilize a legacy biller integration
15 system (BIS) 122 to send batch billing statements to FSC 102 for presentment to
16 and payment by consumers 104(a)...(n). According to one innovative aspect of
17 the invention, billers 106(a-n) incorporating the teachings of the present invention
18 may utilize a "thin" batch billing schema, to be described more fully below.
19 Examples of innovative EBPP systems incorporating BIS technology are provided
20 in U.S. Patent Application No. 08/734,518 to Remington, et al. described above;
21 U.S. Patent Application No. 08/YYYY,YYY to Campbell, et al., entitled *System and*
22 *Method for Designing Responses for Electronic Billing Statements*; U.S. Patent
23 Application No. 08/ZZZ,ZZZ to Dent, et al., entitled *Consumer-Based System and*
24 *Method for Managing and Paying Electronic Billing Statements*; U.S. Patent No.
25 08/880,125 to Campbell, et al., entitled *System and Method for Designing and*
Distributing Customized Electronic Billing Statements; U.S. Patent Application
No. 08/BBB,BBB to Heindel, et al., entitled *Distributed Electronic Billing System*

1 with Gateway Interfacing Biller and Service Center; and U.S. Patent Application
2 No. 08/CCC,CCC to Keith, et al., entitled *Parcel Manager for Distributed*
3 *Electronic Billing System* the disclosures all of which being expressly incorporated
4 herein by reference.

6 **Example Secure Third-party Content Development Systems**

7 **Figs 2A and 2B** illustrate two embodiments of a secure third-party content
8 development system 116 suitable for use within FSC 102 in accordance with
9 teachings of the present invention. With respect to Fig. 2A, secure third-party
10 development system 116 is shown comprising operational controller 202, content
11 development interface 204, validation agent 206, network consumer interface(s)
12 210, memory 212 and, optionally, applications(s) 214, operatively coupled as
13 depicted. It is to be appreciated that although depicted as separate functional
14 elements in a hardware paradigm, one or more of the elements may well be
15 combined (e.g., content development interface 204 and validation agent 206) and
16 these innovative functions may well be implemented (in whole or part) in software
17 executing on computing platform.

18 Third-party development of content depends heavily on the operational
19 controller 202 to enable publishing of content, testing of content prior to
20 production publication and overall management of a biller's presence on FSC 102.
21 The operational controller 202 provides a biller administrator to manage the
22 content development process on FSC 102. In this regard, operational controller
23 202 establishes a biller development account locally, to manage one or more third-
24 party access accounts. For each biller development account, operational controller
25 202 establishes and manages one or more third-party development accounts,
directories and access control lists (ACLs) established on content development
interface 204 and production interface 208. In addition, the operational controller

1 202 receives client certifications (or “certs”) for each third-party developer
2 authorized by the biller to access secure development system 116, and maps such
3 certs to ACLs on the content development interface 204 and the production
4 interface 208. Moreover, once development is complete and the resulting content
5 has been validated by validation agent 206, operational controller 202 receives and
6 maps network address(es) associated with publication of the content (e.g., uniform
7 resource locator (URL) addresses to the content web page) to a database of such
8 network addresses, facilitating further testing and publication of the content.

9 Content development interface 204 provides a staging environment within
10 secure development interface 116 where a developer can store content under
11 development. In this regard, according to one embodiment, content development
12 interface 204 is comprised of a hierarchy of directories roughly denoting a stage of
13 development of content stored within the directories. According to one
14 embodiment, content development interface 204 includes a “working” directory, a
15 “validation” directory, and a “publication” directory. The working directory is
16 where content under active development is maintained. Content that is ready for
17 validation testing by validation agent 206 is moved to the validation directory.
18 Content that is validated by validation agent is maintained in the publication
19 directory until it is moved to the production interface 208 for publication. It
20 should be appreciated that operational controller 202 limits access to the content of
21 any directory to only those with a valid cert to access that content, i.e., currently
22 authorized third-party developers, and FSC 102 technical/administrative support.

23 According to one aspect of the present invention, secure development
24 system 116 includes an automated validation agent 206. It will be appreciated by
25 those skilled in the art that there is a significant risk inherent in allowing third-
parties to develop and publish content from FSC 102. A number of businesses,
financial institutions and consumers rely on the integrity and security of the

1 system. To address the concern of unauthorized access, secure development
2 system 116 relies on registered certs to identify authorized development platforms
3 (computer systems) for each biller development account. To address the concern
4 of rogue or error-laden content bringing down the FSC 102, secure development
5 system 116 utilizes an automated validation agent 206 to analyze the content
6 before it is authorized for publication from FSC 102. In this regard, validation
7 agent 206 analyzes a number of attributes of the developed content to ensure it is
8 safe for publication.

9 Production interface 208 contains validated content created by third-party
10 developers and FSC developers for testing and publication through FSC 102. In
11 this regard, production interface 208 may be regarded as a file server storing and
12 deploying content to consumers via one or more network consumer interface(s)
13 210. As with content development interface 204, content stored on production
14 interface 208 is managed in working, validation and publication directories. The
15 validation directory contains content with a limited publication, e.g., for consumer
16 testing. Content in the publication directory is propagated to one or more network
17 consumer interface(s) 210, which provide access portals to FSC 102 for consumers
18 104. According to one embodiment, consumer network interface(s) 210 are web
19 servers.

20 Fig. 2B illustrates an alternate embodiment of example secure third-party
21 development system 116. In accordance with network diagram of Fig. 2B, secure
22 development system 116 is comprised of a distributed network of servers
23 implementing the features and functions described above. Accordingly, the
24 reference identifiers used in Fig. 2A map to their functional equivalent in Fig. 2B.

25 **Fig. 3** illustrates an example computer system suitable for use as FSC 102
within the data network of Fig. 1. As used herein, but for the innovative secure
development system 116, introduced above, computer system 102 is intended to

1 represent any of a wide variety of general or special purpose computing platforms
2 which implement the teachings of the present invention. It is to be appreciated
3 that the following description of computer system 102 is intended to be merely
4 illustrative, as computer systems of greater or lesser capability may well be
5 substituted without deviating from the spirit and scope of the present invention.

6 As shown, computer 102 includes one or more processors or processing
7 units 132, a system memory 134, and a bus 136 that couples various system
8 components including the system memory 134 to processors 132.

9 The bus 136 represents one or more of any of several types of bus
10 structures, including a memory bus or memory controller, a peripheral bus, an
11 accelerated graphics port, and a processor or local bus using any of a variety of
12 bus architectures. The system memory includes read only memory (ROM) 138
13 and random access memory (RAM) 140. A basic input/output system (BIOS) 142,
14 containing the basic routines that help to transfer information between elements
15 within computer 102, such as during start-up, is stored in ROM 138. Computer
16 102 further includes a hard disk drive 144 for reading from and writing to a hard
17 disk, not shown, a magnetic disk drive 146 for reading from and writing to a
18 removable magnetic disk 148, and an optical disk drive 150 for reading from or
19 writing to a removable optical disk 152 such as a CD ROM, DVD ROM or other
20 such optical media. The hard disk drive 144, magnetic disk drive 146, and optical
21 disk drive 150 are connected to the bus 136 by a SCSI interface 154 or some other
22 suitable bus interface. The drives and their associated computer-readable media
23 provide nonvolatile storage of computer readable instructions, data structures,
24 program modules and other data for computer 102.

25 Although the exemplary environment described herein employs a hard disk
144, a removable magnetic disk 148 and a removable optical disk 152, it should be
appreciated by those skilled in the art that other types of computer readable media

1 which can store data that is accessible by a computer, such as magnetic cassettes,
2 flash memory cards, digital video disks, random access memories (RAMs) read
3 only memories (ROM), and the like, may also be used in the exemplary operating
4 environment.

5 A number of program modules may be stored on the hard disk 144,
6 magnetic disk 148, optical disk 152, ROM 138, or RAM 140, including an
7 operating system 158, one or more application programs 160 including, for
8 example, the innovative secure development system 116 incorporating the
9 teachings of the present invention, other program modules 162, and program data
10 164 (e.g., administrative and transactional information). A user may enter
11 commands and information into computer 102 through input devices such as
12 keyboard 166 and pointing device 168. Other input devices (not shown) may
13 include a microphone, joystick, game pad, satellite dish, scanner, or the like.
14 These and other input devices are connected to the processing unit 132 through an
15 interface 170 that is coupled to bus 136. A monitor 172 or other type of display
16 device is also connected to the bus 136 via an interface, such as a video adapter
17 174. In addition to the monitor 172, personal computers often include other
18 peripheral output devices (not shown) such as speakers and printers.

19 As shown, computer 102 operates in a networked environment using
20 logical connections to one or more remote computers, such as a remote computer
21 176. The remote computer 176 may be another personal computer, a personal
22 digital assistant, a server, a router or other network device, a network "thin-client"
23 PC, a peer device or other common network node, and typically includes many or
24 all of the elements described above relative to computer 102, although only a
25 memory storage device 178 has been illustrated in Fig. 2.

As shown, the logical connections depicted in Fig. 2 include a local area
network (LAN) 180 and a wide area network (WAN) 182. Such networking

1 environments are commonplace in offices, enterprise-wide computer networks,
2 Intranets, and the Internet. In one embodiment, remote computer 176 executes an
3 Internet Web browser program such as the "Internet Explorer" Web browser
4 manufactured and distributed by Microsoft Corporation of Redmond, Washington
5 to access and utilize online services.

6 When used in a LAN networking environment, computer 102 is connected
7 to the local network 180 through a network interface or adapter 184. When used
8 in a WAN networking environment, computer 102 typically includes a modem 186
9 or other means for establishing communications over the wide area network 182,
10 such as the Internet. The modem 186, which may be internal or external, is
11 connected to the bus 136 via a input/output (I/O) interface 156. In addition to
12 network connectivity, I/O interface 156 also supports one or more printers 188. In
13 a networked environment, program modules depicted relative to the personal
14 computer 102, or portions thereof, may be stored in the remote memory storage
15 device. It will be appreciated that the network connections shown are exemplary
16 and other means of establishing a communications link between the computers
17 may be used.

18 Generally, the data processors of computer 102 are programmed by means
19 of instructions stored at different times in the various computer-readable storage
20 media of the computer. Programs and operating systems are typically distributed,
21 for example, on floppy disks or CD-ROMs. From there, they are installed or
22 loaded into the secondary memory of a computer. At execution, they are loaded at
23 least partially into the computer's primary electronic memory. The invention
24 described herein includes these and other various types of computer-readable
25 storage media when such media contain instructions or programs for implementing
the innovative steps described below in conjunction with a microprocessor or
other data processor. The invention also includes the computer itself when

1 programmed according to the methods and techniques described below.

2 Furthermore, certain sub-components of the computer may be programmed to
3 perform the functions and steps described below. The invention includes such
4 sub-components when they are programmed as described. In addition, the
5 invention described herein includes data structures, described below, as embodied
6 on various types of memory media.

7 For purposes of illustration, programs and other executable program
8 components such as the operating system are illustrated herein as discrete blocks,
9 although it is recognized that such programs and components reside at various
10 times in different storage components of the computer, and are executed by the
11 data processor(s) of the computer.

12 **Example Content Authoring System**

13 **Figs. 4A and 4B** illustrate example content authoring systems, suitable for
14 the development and publication of content through FSC 102. With reference to
15 Fig. 4A, content authoring system 400 is comprised of one or more development
16 platforms 402(a-n), a gateway billing integration system (BIS) 404 including a
17 prep gateway BIS 406 and a production gateway BIS 408, and one or more user
18 test platforms 410(a-n), operationally coupled as depicted. It will be appreciated
19 that although depicted as separate functional elements according to a hardware
20 paradigm, one or more elements (e.g., prep gateway BIS and production gateway
21 BIS) may well be combined into a single element, and may well be comprised of
22 software functions which, when executed, implement the innovative features
23 described herein.

24 Development platform(s) 402(a-n) represent computing systems suitably
25 endowed with content development software (e.g., FrontPage 2000 introduced
above). According to one embodiment, each development platform 402(a-n) has a
unique cert (not shown), which must be registered and have current authoring

1 privileges in order to utilize the features of secure development system 116.

2 According to one embodiment, offline development is supported wherein the
3 developer downloads FSC implemented objects to development system 402 to
4 develop customized content, e.g., an application server page providing
5 Registration, Support, eForms, etc. Once local coding of the ASP is complete, the
6 content is moved to secure development platform 116 from a development system
7 with a current cert, to continue the validation and publication process.

8 As introduced above, the gateway BIS 404 provides a means of integrating
9 legacy billing systems with FSC 102, enabling billers to leverage the legacy
10 billing systems and data for use with the innovative FSC 102. A detailed
11 description of the BIS is provided in the above referenced co-pending applications,
12 which are included herein by reference.

13 The user test platforms 410(a-n) are intended to represent any of a number
14 of computer systems 114 that a consumer may use to access and utilize the
15 features of FSC 102. In this implementation as a test platform 410, the computer
16 systems execute a test sequence designed to identify latent defects in the
17 developed content. The user test platforms 410 access content located in the
18 validate directory of the production interface 208 in performing this valuable
19 function. Once the user test platforms 410 have satisfactorily completed their test
20 sequences, the third-party developed content is promoted to the publication
21 directory, and propagated to one or more web servers 210(a-n).

22 Fig. 4B illustrates an alternate embodiment of example content authoring
23 system 400. In accordance with network diagram of Fig. 4B, content authoring
24 system 116 is comprised of a distributed network of computing systems
25 implementing the features and functions described above. Accordingly, the
reference identifiers and description associated the elements of Fig. 4A map to
their functional equivalent in Fig. 4B.

1 **Fig. 5** is a block diagram of an example computing device 402 suitable for
2 use as a content authoring platform, according to one embodiment of the present
3 invention. As shown, computing device 402 includes one or more processing
4 unit(s) 502, a non-volatile memory device 504, a display device 506, an input
5 device 508, input/output (I/O) port(s) 510, volatile system memory 512 and a
6 storage device 514 including a content development application 516 (e.g.,
7 FrontPage 2000) which, when executed, enables a developer to generate content
8 for publication via FSC 102.

9 As described above, except for its interaction with secure third-party
10 development system 116 in developing publishable content for FSC 102, computer
11 system 102 is intended to represent a wide variety of computing devices known in
12 the art. Similarly, the functional blocks 402-426 are each intended to represent
13 any of a plurality of devices that perform these functions and, thus, need not be
14 described further.

15 **Example Data Structure**

16 **Fig. 6** graphically illustrates an example data structure 118 suitable for use
17 with secure development system 116 and FSC 102. As shown, data structure 118
18 is comprised of a number of fields including one or more of a user_ID field 602,
19 password information field 604, one or more financial institution account numbers
20 606, one or more authentication code fields 608(a-n), a billing summary filename
21 field 610 and a field containing a path to detailed billing information (Detail_path)
22 612. It will be appreciated that, data structures 118 of greater or lesser complexity
23 may well be used without deviating from the spirit of the present invention.

24 As used herein, the user_ID field 602 and the password information field
25 604 enable FSC 102 to verify the identity and authenticity of a user requesting
access to an account. In this regard, the user_ID/password combination must be

1 unique to a single individual. A number of user_ID and password criteria may be
2 used to satisfy the uniqueness criteria. In one implementation, for example, a
3 user's Microsoft Passport ID (email address/password combination) are used to
4 uniquely identify the individual. Although not shown, the data structure 118 may
5 also contain fields for additional user information such as, for example, an
6 address, a telephone number, and/or additional credit history information (not
7 shown).

8 The financial institution account numbers 606 provide a link to the asset-
9 backed accounts of a bank, brokerage, etc., that store the financial assets to cover
10 the financial transactions of the user. In this regard, the financial institution (FI)
11 accounts are intended to represent any of a wide variety of such accounts known in
12 the art including, but not limited to, savings accounts, checking accounts, money
13 market accounts, brokerage accounts and the like. In one embodiment, the email
14 system 102 provides its users with an FI account (i.e., an integrated email/FI
15 account), enabling users to deposit and withdraw funds from the email account
16 itself.

17 According to one aspect of the invention, the authentication codes 608(a-n)
18 are used to provide the seamless integration of FSC 102 hosted content with
19 content hosted by the biller 106, or some other third party (e.g., a technical support
20 consultant). To provide automated redirection to and authentication at a billers
21 site, consumer user interface 120 (authored by FSC or some third-party) is
22 configured to transmit the authentication codes (or equivalents) to the billers
23 computing system. According to one implementation, the authentication codes are
24 supplied to FSC 102 along with summary bill information in a batch billing
25 statement downloaded to FSC (according to the thin batch bill schema introduced
above). In an alternate embodiment, the use of authentication codes is eliminated
through the use of a dual sign-in procedure, wherein the user first signs on to the

1 FSC 102, and then must subsequently sign on to the biller's computing system 106
2 when redirected for display of detailed bill data (for example).

3 The summary bill file field 610 identifies the name of a file wherein
4 summary bill data for the associated account is found. According to one
5 implementation, this information is provided in the batch billing statement and
6 stored in a file on FSC 102. In an alternate embodiment, summary bill file field
7 610 includes path information to identify a remotely located file containing the
8 summary bill information.

9 The detail_path field 612 identifies the path to detailed billing information.
10 According to the teachings of the present invention, introduced above, the detailed
11 billing information may well be hosted on a remote, third-party server (e.g.,
12 associated with the billers computing system 106).

14 **Example Operation and Implementation**

15 Having introduced the architectural and functional elements of the present
16 invention with reference to Figs. 1-6, the operation secure third-party development
17 system 116 and implementations of biller authored and/or hosted content is
18 presented with reference to the remaining Figs. 7-15.

19 **Example Third-party Content Development**

20 **Fig. 7** illustrates a flow chart of an example method for secure third-party
21 development of FSC content, according to one embodiment of the invention. As
22 shown, the method begins with block 702, wherein a biller development account is
23 created on secure development system 116. More specifically, a biller
24 administrator accesses ops server 202 to establish a biller development account.
25 In response, ops server 202 creates development accounts, directories and updates
access control lists (ACLs) on staging server 204 to facilitate such development.
Before a developer can begin using the secure development system 116, however,

1 biller administrator must add the certs uniquely identifying authorized third-party
2 developers to the ACLs.

3 In block 704, third-party developers save developed content to appropriate
4 directories in development system 116. That is, depending on the stage of
5 development, a third-party content developer saves their developed content in a
6 working, validation or publication directory of staging server 204. According to
7 one embodiment, staging server 204 includes the working, validation and
8 publication directories for each of a number of FSC supported applications such
9 as, for example, Registration services, Support services, electronic Forms content,
10 and the like.

11 In block 706, once initial coding is completed, the developed content is
12 promoted from the working directory to a validation directory to facilitate
13 validation testing of the third-party developed content. As introduced above,
14 secure development system 116 invokes an instance of automated validation agent
15 to automatically identify errors in the third-party developed code. According to
16 one embodiment, automated validation agent 206 analyzes the developed content
17 for ASP errors, and other objects the execution of which could compromise FSC
18 102, other billers 106, or consumers 104.

19 In block 708, validation agent 206 determines whether the analyzed content
20 is acceptable. If not, the third-party developer (e.g., 126) and/or associated biller
21 106 is notified, and development continues to eliminate the identified errors with
22 block 710.

23 If, in block 708 validation agent determines that the developed content is
24 acceptable, the content is propagated to a working directory for that content on the
25 production server 208, which also populates one or more web server(s) with the
content for consumer testing. Before further consumer validation testing may be
performed, ops server 202 must be given network address(es) to map to the newly

1 developed content, block 714. In response, ops server 202 provides the network
2 address information to SQL server 212, which updates its database of network
3 addresses.

4 In block 716, simulated consumer testing is performed by user test
5 platforms 410(a-n) to identify any latent problems that a consumer might
6 encounter using the third-party developed content. If problems are identified,
7 block 718, the files are automatically removed from the production and web
8 servers, as the debug process continues from the working directory of the staging
9 204 or production 208 servers. Note, validation testing of modified content may
10 be required before the developed content can be promoted to and propagated from
11 the production server 208, or before additional consumer testing.

12 If, in block 718, the consumer testing of the developed content failed to
13 identify any errors, the developed content is promoted to the publication directory
14 of the production server 208, and is ready for production status at the authorization
15 of the biller administrator. According to certain implementations, additional
16 manual controls may restrict production publication of newly developed third-
17 party content until FSC technical/administrative staff have manually reviewed the
18 content, e.g., using consumer test platforms 410.

19 In block 724, upon successful development and validation of content (722),
20 ops server 202 determines whether development for the associated biller is
21 complete. According to one embodiment, ops server 202 will prompt biller 106
22 with a question of whether to extend the authorization of biller development
23 account (and associated certs). If, in block 724 ops server determines that
24 development is not complete, the development process continues with block 710.

25 If, in block 724, development is complete, ops server 202 disables the biller
development account and breaks all cert mapping, block 726. According to one
embodiment, ops server changes the password and privileges associated with the

1 biller development account, forestalling any further access by biller or associated
2 third party developers. In addition, ops server 202 removes the associated certs
3 from ACLs associated with the biller.

4 **Fig. 8** graphically illustrates an example graphical user interface (GUI),
5 projected by ops server 202, facilitating management of secure development
6 system 116. As shown, GUI 800 is a web page projected by an ops server 202 of
7 secure development system 116 with links to invoke one or more of the functions
8 discussed above. According to the illustrated example embodiment, GUI 800
9 includes links to enable a biller administrator to change their ops site password
10 (802), register a publishing cert (804) for a third-party developer, customize the
11 site (806) with developed content (e.g., Registration services, Support services,
12 Bill presentment, etc.), and to debug (validate) (808) developed content.

13 **Fig. 9** illustrates a GUI facilitating publication of a cert, projected to a biller
14 administrator in response to selection of link 804. According to the illustrated
15 embodiment, ops server 202 instructs an operating system of development
16 platform 402 to project a user interface denoting the certs associated with the
17 platform 402. GUI 900 allows the user to select an appropriate cert, if more than
18 one is available, for use with secure development system 116. GUI 902 is
19 displayed once a valid cert is provided and registered with ops server 202.

20 **Fig. 10** graphically illustrates a GUI 1000 enabling an authorized biller
21 administrator to customize the biller's FSC site, according to one embodiment of
22 the present invention. As shown, the GUI 1000 enables a user to identify and
23 enable customized registration and support content, in addition to the bill detail
24 content.

25 **Fig. 11** illustrates a flow chart of an example method for validating third-
party developed content, according to one embodiment of the invention. As
shown, the method begins with invocation of validation agent 206 by a developer

1 or biller administrator, block 1102. In block 1104, validation agent 206 analyzes
2 code comprising the third-party content for conflicts, ASP errors, security
3 problems, etc., and makes a determination in block 1106 whether the content is
4 technically error free.

5 If the content contains errors, validation agent 206 generates a report
6 identifying failing content files and the location and cause of the failure. In
7 addition, as introduced above, validation agent 206 deletes the files from the
8 validation directory of the staging server 204.

9 If, in block 1106, validation agent 206 determines that the third-party
10 content is free from ASP and other errors, validation agent 206 instructs the user
11 that the content passed validation testing. According to one embodiment,
12 validation agent will prompt the developer or biller administrator whether they
13 wish to promote the validated files to the production server and propagate the files
14 to the web server(s), block 1112. If so, the files are so promoted and propagated
15 by validation agent.

16 According to an alternate embodiment, validation agent 206 automatically
17 performs file management services, promoting validated files to the production
18 server for propagation and deleting the files from the validation directory. Such an
19 embodiment provides for improved file management practices, lessening the
20 probability that stale files are forgotten in the validation directory.

21 **Fig. 12** is a flow chart illustrating a method for biller authored and hosted
22 content, according to one embodiment of the present invention. As shown, the
23 method begins with block 1202, wherein the biller 106 creates one or more
24 authentication strings associated with each bill to be submitted to FSC 102 in a
25 batch billing statement. The created strings are stored locally in a billing database
(not shown) maintained by the biller system.

1 In block 1204, the batch billing data including at least a representation of
2 the authentication strings is sent to FSC 102. According to one embodiment,
3 introduced above, the batch billing data adheres to a thin batch billing schema,
4 wherein minimal information is provided to the FSC 102 in the batch billing
5 statement, thereby reducing the amount of confidential information is transmitted
6 outside biller system 106. According to one embodiment, only a biller identifier,
7 summary bill data including a consumer identifier, and the authentication codes
8 are sent in the thin batch billing schema.

9 In block 1206, FSC 102 receives the batch billing data and populates
10 transactional records in storage device 118. More specifically, with reference to
11 Fig. 6, for each consumer ID/Biller ID combination, a record 614 is entered into
12 data structure 118.

13 In block 1208, a requesting registered user is provided with minimal bill
14 detail in an FSC generated summary page. From this summary page, the
15 registered user could pay the bill, completing the transaction without any further
16 review of bill data. If, in block 1210, the user requests detailed bill information,
17 the summary page (authored either by FSC 102, biller 106, or third-party
18 developer 126 to denote biller hosted bill-detail), FSC 102 redirects the user's
19 browser to billers system 102 providing the authentication codes as a means of
20 authenticating the registered user's access to the requested detailed billing
21 information, block 1212. According to one embodiment of the invention, the
22 redirection to and authentication with the billers system is hidden from the view of
23 the registered user. According to one implementation, FSC 102 provides the user
24 with an indication that the requested information is being retrieved.

25 If, in block 1214, billers system is unable to authenticate the registered user
given the provided authentication strings, billers system 106 rejects the access
request, and FSC 102 provides the user with an error message.

1 Alternatively, if billers system 106 authenticates the registered user, a
2 composite billing user interface is generated comprising FSC generated content
3 and biller generated content, block 1218.

4 **Fig. 13** provides an architectural dependency perspective on biller authored
5 and biller hosted content, according to the teachings of the present invention. As
6 shown, FSC 102 minimally provides navigation aids 1204, e.g., a top
7 navigation/function bar and a left navigation/function bar. In the biller authored
8 model, at least a subset 1202 of the content is developed by biller 106. In one
9 embodiment, the content may be authored by a third-party developer but stored
10 and projected by FSC 102. Alternatively, FSC 102 and billers site 106 may
11 cooperatively work to provide composite content including an FSC authored and
12 hosted component (1204) and a biller authored and hosted component 1202.

13 **Fig. 14** graphically represents an example bill summary user interface (UI)
14 1400, according to one embodiment of the present invention. As shown, the UI
15 includes a top navigation/function bar 1402 and a left navigation/function bar
16 1404. As introduced above, these elements are authored and hosted by FSC 102.
17 In addition, UI 1400 includes lower frame 1406, which includes an advertising
18 banner 1408 and bill summary information 1410. According to one embodiment,
19 the lower frame 1406 is authored by biller 106, but hosted from FSC 102. There
20 may be a number of advantages to hosting summary pages from FSC 102. First,
21 by hosting summary page UI 1400 from FSC 102, it protects the consumer (and
22 the biller) from an unavailable biller computer system. That is, if the biller system
23 106 goes down, a consumer would be unable to access their account with biller. If
24 the information is hosted by FSC 102, if the biller computer system 106 goes
25 down, the consumer can still complete payment transactions without having to
access the billers site (e.g., to review detailed information).

1 **Fig. 15** graphically illustrates an example detailed billing user interface
2 1500 with an FSC-hosted component and a biller-hosted component, according to
3 one embodiment of the present invention. As shown, the navigation/function bars
4 1402 and 1404 are hosted from FSC 102, while the detailed bill information 1502
5 is hosted from billers computer system 106.

6 It is to be appreciated, given the foregoing discussion, that the innovative
7 secure third-party development system 116 facilitates third-party authoring and/or
8 hosting of content via FSC 102. Although the invention has been described in
9 language specific to structural features and/or methodological steps, it is to be
10 understood that the invention defined in the appended claims is not necessarily
11 limited to the specific features or steps described. Rather, the specific features and
12 steps are disclosed as exemplary forms of implementing the claimed invention.